AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

initializing a pseudo-random number generator (PRNG);

obtaining local seeding information from a host;

securely obtaining ~~additional~~ remote seeding information from ~~one or more~~ remote entropy servers ~~using~~ via a secure entropy collection protocol, the remote seeding information to be mixed with the local seeding information to perform one or more of providing an unpredictable system status, amplifying entropy, and enhancing system security;

repeating ~~wherein~~ the securely obtaining of the ~~additional~~ remote seeding information ~~is repeated~~ for each entropy server~~, wherein the secure entropy collection protocol is to perform:~~;

generating a key pair including a temporary asymmetric public key and a temporary asymmetric private key[[,]];

encrypting the temporary public key with a public key associated with a remote entropy server[[,]];

decrypting the temporary public key with a private key associated with the remote entropy server[[,]];

encrypting the ~~additional~~ remote seeding information with the temporary public key~~, and~~;

decrypting the ~~additional~~ remote seeding information with the temporary private key; and

stirring the PRNG via the local seeding information and the ~~additional~~ remote seeding information.

2. (Previously Presented) The method of claim 1, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

3. (Previously Presented) The method of claim 2, wherein the random value comprises a seed.

4. (Cancelled)

5. (Currently Amended) The method of claim 1, wherein the ~~one or more~~ remote entropy servers maintain random state pool to supply the host with the random value.

6. (Currently Amended) The method of claim 1, wherein the ~~securely~~ obtaining of the remote seeding information from the ~~one or more~~ remote entropy servers ~~includes using~~ is performed via a privacy protocol.

7. (Original) The method of claim 6, wherein the privacy protocol comprises secure sockets layer (SSL) protocol.

8. (Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Previously Presented) The method of claim 1, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.

Claims 10-16 (Cancelled)

17. (Currently Amended) An entropy enhancing system comprising:

~~a local system including a host and a pseudo-random number generator (PRNG),~~ ~~the local system to~~

a host at a local computer system coupled with remote entropy servers at remote computer systems; and

a server computer system coupled with the local computer system and the remote computer systems, the server to

initialize ~~the PRNG~~ a pseudo-random number generator (PRNG) by obtaining local seeding information from the host,

securely obtain ~~additional~~ remote seeding information from ~~one or more~~ the remote entropy servers ~~using~~ via a secure entropy collection protocol, the remote seeding information to be mixed with the local seeding information to perform one or more of providing an unpredictable system status, amplifying entropy, and enhancing system security,

repeating ~~wherein~~ the securely obtaining of the ~~additional~~ remote seeding information ~~is repeated~~ for each entropy server~~, the secure entropy collection protocol is to perform:~~,

~~generating~~ generate a key pair including a temporary asymmetric public key and a temporary asymmetric private key,

~~encrypting~~ encrypt the temporary public key with a public key associated with a remote entropy server,

~~decrypting~~ decrypt the temporary public key with a private key associated with the remote entropy server,

~~encrypting~~ encrypt the ~~additional~~ remote seeding information with the temporary public key, ~~and~~

~~decrypting~~ decrypt the ~~additional~~ remote seeding information with the temporary private key[[;]], and

stir the PRNG via the local seeding information and the ~~additional~~ remote seeding information.

18. (Currently Amended) The entropy enhancing system of claim 17, wherein the local computer system ~~generates~~ to generate the local seeding information ~~at the host~~ via the host.

19. (Currently Amended) The entropy enhancing system of claim 17, wherein the ~~one or more~~ remote computer systems ~~generates~~ are to generate the remote seeding information ~~at the one or more~~ via the remote entropy servers.

Claims 20-24 (Cancelled)

25. (Currently Amended) A machine-readable medium having ~~stored thereon data representing sets of~~ instructions which, when executed ~~by a machine~~, cause ~~the~~ a machine to:

initialize a pseudo-random number generator (PRNG);

obtain local seeding information from a host;

securely obtain ~~additional~~ remote seeding information from ~~one or more~~ remote entropy servers ~~using~~ via a secure entropy collection protocol, the remote seeding information to be mixed with the local seeding information to perform one or more of providing an unpredictable system status, amplifying entropy, and enhancing system security;

repeat ~~wherein~~ the securely obtaining of the ~~additional~~ remote seeding information ~~is repeated~~ for each entropy server~~, wherein the secure entropy collection protocol is to:~~;

generate a key pair including a temporary asymmetric public key and a temporary asymmetric private key[[,]];

encrypt the temporary public key with a public key associated with a remote entropy server[[,]];

decrypt the temporary public key with a private key associated with the remote entropy server[[,]];

encrypt the ~~additional~~ remote seeding information with the temporary public key~~, and~~;

decrypt the ~~additional~~ remote seeding information with the temporary private key; and

stir the PRNG via the local seeding information and the ~~additional~~ remote seeding information.

26. (Currently Amended) The machine-readable medium of claim 25, wherein the instructions when executed to ~~initializing of~~ initialize the PRNG ~~comprises~~ further cause the machine to ~~initializing~~ initialize an internal state of the PRNG with a random value.

27. (Previously Presented) The machine-readable medium of claim 26, wherein the random value comprises a seed.

28. (Cancelled)

29. (Currently Amended) The machine-readable medium of claim 25, wherein the ~~one or more remote entropy servers~~ instructions when executed, further cause the machine to maintain random state pool to supply the host with the random value.

30. (Currently Amended) The machine-readable medium of claim 25, wherein the instructions when executed to ~~stirring of~~ stir the PRNG ~~comprises producing~~ further cause the machine to produce a cryptographically random stream of bits.